Department of the Army **FM Supplement 1 to AR 380-5**
Headquarters Fort Monroe
Fort Monroe, Virginia 23651-5000

15 August 2006

Security
DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM

Summary. This supplement provides local guidance for managing the Department of the Army Information Security Program within Headquarters, Fort Monroe (HQFM).

Applicability. This supplement applies to all military, civilian employees, contractors, tenant units, and activities assigned or attached to HQFM.

Suggested improvements. The proponent of the supplement is the Directorate of Plans, Training, Mobilization, and Security (DPTMS). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, Fort Monroe, ATTN: IMNE-MNR-PLS, Fort Monroe, VA 23651-1110. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

Availability. This publication is available on the Fort Monroe homepage at http://fort.monroe.army.mil.

AR 380-5, 29 September 2000, is supplemented as follows:

Add the following appendices to the table of contents:

J. Emergency Plan for the Protection of Classified Material.
K. Hand carry of Classified Material.
L. Preliminary Inquiries and Security Investigations.

Paragraph 1-2. References

Add the following sentences to paragraph 1-2:

“Security Managers will maintain, at a minimum, the references listed in Appendix A, Section V of this supplement. Hardcopies of these references are not required. Electronic copies may be downloaded and saved to a directory on your computer for reference and inspections. Army regulations may be downloaded from the Army Publishing Directorate (APD) at www.apd.army.mil.

Other referenced material may be requested from the Security Division, DPTMS."

Paragraph 1-3. Explanation of abbreviations and terms

Add the following sentence to the end of paragraph 1-3:

"Unless otherwise specified, the term "Security Manager" refers to unit, activity, and tenant security managers."

Paragraph 1-6. The Commander

Add the following sentence to the end of paragraph 1-6e:

"The HQFM Command Security Manager (CSM) is the Chief, Security Division, DPTMS."

After subparagraph 1-6k, add the following:

"l. Commanders will appoint a primary and alternate security manager in writing and forward a copy of the appointment orders to the Security Division, DPTMS, within 10 days of the appointment. Security managers will schedule an initial security orientation with the Security Division, DPTMS, within 30 days of appointment.

m. Commanders will ensure security managers establish written standing operating procedures (SOP) based on AR 380-5, AR 380-67, this supplement, and other applicable references. Security managers will forward a copy of the SOP to the Security Division, DPTMS, for approval. Security managers will update the SOP annually, as needed, and forward the revised SOP to the Security Division for approval."

Paragraph 1-8. The Supervisor

After subparagraph 1-8c, add the following:

"(1) Supervisors will report to the security manager any information that may have a bearing on an individual's (to include contractor personnel) eligibility for continued access to classified and sensitive information.

(2) Security managers will report to the CSM any information that may have a bearing on an individual's (to include contractor personnel) eligibility for access to classified and sensitive information."

Paragraph 1-9. The Individual

Add the following sentence to the end of paragraph 1-9:

“The security SOP will include procedures for individuals to report security violations.”

Paragraph 1-10. Applicability definition

Add the following sentences to the end of paragraph 1-10:

“In the event that procedures specified in this supplement conflict with the requirements of a tenant, the CSM will contact the MACOM/NERO for resolution. In the interim, the tenant’s MACOM will take precedence.”

Paragraph 1-11. General principles

After subparagraph 1-11e, add the following:

“f. Security managers will submit requests for security clearances and access to the Security Division, DPTMS. Security managers are the sole points of contact with the DPTMS, Security Division for requesting security clearances or access.

(1) The Security Division, DPTMS will provide up-to-date security access rosters to all (applicable) units/activities monthly. The security access roster will be used to verify an individual’s eligibility for access to classified material up to the level indicated on the roster.

(2) The Security Division, DPTMS, will provide a work case roster to applicable security managers monthly. The work case roster will include the names of individuals currently being processed for security access. Security managers are responsible for updating their security access and work case rosters as changes occur.”

Paragraph 1-18. Military Operations, Exercises, and Unit Deactivations

After subparagraph 1-18b, add the following:

“(1) Within HQFM the use of “mock” classified material is authorized in rare instances to meet specific training objectives.

(2) When using “mock” classified material during military exercises, annotate the words **“**CLASSIFIED FOR TRAINING ONLY**”** directly below the overall classification markings.

(3) Protect exercise material marked **“**CLASSIFIED FOR TRAINING ONLY**”** in the same manner as real-world classified material at the same classification level and destroy the material as classified waste at the end of the exercise.”

(4) If real-world classified material is introduced to or used during military training exercises, do not intermingle or store the real-world material with the mock classified material.”

Paragraph 1-22. Reporting of Incidents

Add the following sentence to the end of paragraph 1-22:

“The CSM will forward incident reports to the appropriate MACOM/NERO.”

Paragraph 1-23. Reporting Requirements

Add the following sentences to the end of paragraph 1-23:

“Security managers will report the total number of SECRET and CONFIDENTIAL documents (including electronically transmitted classified messages, and SIPRNET documents) derivatively created to the DPTMS, Security Division (via email) not later than (NLT) the 15th of the month following the end of each quarter, unless requested earlier. The CSM will forward the annual report (SF 311) to the MACOM/NERO no later than 1 September of each year, unless requested earlier. Annual reports will contain consolidated HQFM information for the current fiscal year.”

Paragraph 1-24. Command security inspections

After paragraph 1-24, add the following:

“a. The Security Division, DPTMS will conduct annual command inspections (CI) of units and activities that retain classified material. The inspection will include a review of security containers that store classified material. Security managers of units/activities without classified holdings will conduct annual self-inspections. The Security Division, DPTMS, will notify security managers of command inspections at least 30 days prior to their inspection date. The Security Division, DPTMS, will

provide security managers, who conduct self-inspections, a self-inspection packet at least 30 days prior to the self-inspection period. A copy of reports for each type of inspection will be maintained on file within the unit/activity until the next comparable inspection.

b. Units and activities, to include the tenant, that store classified material are subject to unannounced inspections by the Security Division, DPTMS. The purpose of unannounced inspections is to ensure classified material is properly stored during non-duty hours."

Paragraph 2-3. Delegation of authority

Add the following sentence to the end of subparagraph 2-3a:

"The Commanding General (CG), HQ TRADOC, is the Original Classification Authority (OCA) for HQFM. The clearance level of the OCA is up to SECRET."

Paragraph 2-4. Required Training

Add the following sentence to the end of paragraph 2-4:

"Individuals authorized to assume the position of the delegated OCA, in his/her absence, will also receive this training before exercising such authority."

Paragraph 2-5. Policy

Add the following sentence to the end of paragraph 2-5:

"If the classification is derived from more than one source, the identification of each source by title, originator, classification, page, paragraph, and date will be documented in writing and maintained with the file or record copy of the document."

Paragraph 2-6. Accuracy responsibilities

Add the following sentences to the end of subparagraph 2-6d:

"When extracting information from classified documents without internal markings, contact the original classifier to determine the proper classification of the extracted information. In time sensitive situations, the extracted information will be classified at the same level as the overall source document

classification until specific classification guidance is received. Upon receipt of guidance, all copies of documents containing the extracted information will be re-marked with the appropriate classifications, as required. The extractor is responsible for contacting the original source to obtain the proper classification, marking the extracts, and informing all recipients of the proper classification markings."

Add the following sentence to the end of subparagraph 2-6f:

"When information is derivatively classified by "multiple sources," a listing of all sources will be included with all copies of the document."

Paragraph 2-13. Compilation

Add the following sentences to the end of paragraph 2-13:

"Consult the CSM for guidance concerning whether or not compilation results in classification. A document that becomes classified or that is raised to a higher classification because of compilation will have a caveat supporting the higher classification. In all cases, the OCA's decision is required. The caveat will:

After paragraph 2-13, add the following:

"a. Cite the authority that classified the document or raised the classification of the document.

b. State which part(s) of the new document constitutes the compilation.

c. Include the appropriate declassification instructions."

Paragraph 2-16. Policy

Add the following sentences to the end of paragraph 2-16:

"Units and activities involved in the planning of classified exercises will ensure that adequate classification guidance is provided to all exercise participants. Classification guidance may be published as a separate document or incorporated into exercise plans or directives."

At the end of paragraph 2-16, add the following:

“a. After a Security Classification Guide (SCG) is approved, it may be used as the classification authority for documents containing the type of information covered in the guide.

b. Documents deriving their classification from an approved SCG need not have approval of the OCA. These documents will cite the SCG as the classification authority.”

Paragraph 3-1. General

After subparagraph 3-1d, add the following:

“f. Security Managers will submit requests to declassify or downgrade classified files to the CSM for review.

g. The CSM will submit the request to the OCA for review for declassification determination.”

Paragraph 3-2. Special Program Manager

After subparagraph 3-2c, add the following:

“d. Security managers will establish procedures to ensure that all classified material is reviewed for declassification or exemption determination, prior to the date of automatic declassification.”

Paragraph 3-5. General

After subparagraph 3-5b, add the following:

“c. Classified files and records that are more than 25 years old will not be automatically declassified without being reviewed to determine if continued classification is warranted or authorized.”

Paragraph 3-9. General

After subparagraph 3-9b, add the following:

“c. Security managers will establish procedures to ensure that periodic reviews are conducted for classified documents that have been exempted from the 25 year automatic declassification requirement to determine continued need for classification.”

Paragraph 3-10. Downgrading information

Add the following sentence to the end of paragraph 3-10:

“Requests to downgrade or declassify information will be submitted to the CSM for review.”

Paragraph 3-14. Concepts of destruction

Add the following sentence to the end of paragraph 3-14:

“Security managers will employ the “secure volume” concept to destroy classified material with GSA approved shredders.”

Paragraph 3-15. Approved routine methods of destruction

Add the following sentences to the end of subparagraph 3-15b:

“Shredders used to destroy classified material will be approved, in writing, by the CSM or designee. All shredders not approved for the destruction of classified material will be labeled. The use of commercial (contract) shredding companies to destroy classified material is prohibited. The use of commercial (Contract) shredding companies to destroy unclassified/sensitive information will be requested thru the Security Division, DPTMS for review and decision.”

Paragraph 4-4. Overall classification marking

After paragraph 4-4, add the following:

“a. Mark or stamp classified documents without a back cover with the overall classification of the document at the top and bottom, and on the back of the last page, as an additional security measure against possible compromise.

b. Mark or stamp by-hand classification markings, warning notices, caveats, releasability, and declassification/ downgrading instructions to ensure legibility when not clearly visible on reproduced copies. Apply all classification and associated markings in black ink.”

4-6. Page and portion marking

Add the following sentence to the end of subparagraph 4-6b:

“Within HQFM, mark each subparagraph to show the level of classification.”

4-22. File, folders, and groups of documents

After paragraph 4-22, add the following:

“a. Coversheets may be left on documents placed in a security container under the following circumstances:

(1) When a document is placed in a suspense file;

(2) When a document or file is being used daily and is kept in a hold box, hold file or folder, within the container when not needed;

(3) When permanently affixed to the outside front and back of hard cover binder or other container where the classification markings cannot be adequately or legibly stamped thereon;

b. Conspicuously mark binders containing classified documents on the front and back covers and on the spine, with the highest level of classified information contained therein;

c. Mark or stamp file folders containing classified information top and bottom, front and back, with the highest classification of the information contained therein.”

4-23. Printed documents produced by AIS equipment

After subparagraph 4-23c, add the following:

“d. Review classified products produced on an Automated Information Systems (AIS) to ensure the material has the proper classification markings and instructions, prior to electronic transmission or printing.”

4-28. Slides and transparencies

Add the following sentences to the end of subparagraph 4-28b:

“Mark each remaining slide in the set with its security classification or “Unclassified.” A slide separated from the set and subsequently handled apart from the set will be marked with its classification and the applicable associated markings or the marking of “Unclassified” as required.”

4-32. Removable AIS storage media

After subparagraph 4-32c, add the following:

“d. Classified information contained on fixed or removable magnetic storage media must be stored in an authorized classified container or in a facility approved for the open storage of classified material. Refer to AR 25-2, Information Assurance, for further guidance.”

5-3. Marking

After subparagraph 5-3b(4), add the following:

“(5) When authorized, FOUO documents or materials released to agencies outside the Department of Defense will contain the following additional expanded marking on the front cover or first page:

“This document/material contains information exempt from mandatory disclosure to the public under the Freedom of Information Act. Exemption (indicate exemption(s) specified in AR 25-55) applies.”

(6) FOUO documents or materials, as well as all other controlled unclassified information (CUI), require the consent of the originator or proponent before disclosing to foreign governments or representatives. Refer to AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, for further guidance.”

After paragraph 5-24, add the following:

“Section VI
Law Enforcement Agency Sensitive Information

5-25. Description
Law Enforcement Agency (LEA) Sensitive Information is unclassified information that is originated by various local, state, and federal law enforcement agencies and requires protection against unauthorized disclosure in order to protect sources and methods of criminal activities, investigations, and evidence.”

5-26. Marking

a. Unclassified documents or materials containing LEA sensitive information will be marked “LEA SENSITIVE” in letters larger than the rest of the text, where practical, at the top and bottom of the front cover, the title page, the outside of the back cover, and on each page containing LEA sensitive information.

b. Classified documents containing LEA sensitive information will be marked as required in AR 380-5, Chapter 4, except pages containing LEA sensitive information, but no classified information, will be marked “LEA SENSITIVE” top and bottom.”

5-27. Access to LEA sensitive information

Access to LEA sensitive information will be granted to persons who have a valid need-to-know. A security clearance is not required. LEA information will not be released outside the Department of Defense without prior authorization by the originating LEA.”

5-28. Protection of LEA sensitive information

a. To the maximum extent possible, transmit LEA sensitive information via secure means, store in a locked container, disseminate only when the need-to-know of the recipient has been established, and shred when no longer needed. LEA sensitive information may be processed on unclassified computers and local area networks. Do not store data on a system accessible via the internet that does not have approved firewall protection. In the absence of secure transmission capabilities, the information may be transmitted over unsecured facsimile machines.

b. When mailing LEA sensitive information, double wrap and send via First-Class mail.

c. Store LEA sensitive information in a locked container. A GSA-approved security container is not required.

d. Keep the reproduction of LEA sensitive information to a minimum and limit to operational necessity.

e. When no longer needed, shred LEA sensitive information.”

6-1. Responsibilities

After paragraph 6-1, add the following:

“a. Individuals will not allow access to classified material until, need-to-know, appropriate security clearance, and access is verified.

(1) Collecting, obtaining, recording, or removal of classified material for personal use is prohibited.

(2) Release of classified material to foreign nationals, governments, and international organizations is prohibited until a Delegated Disclosure Authority (DDA) has determined that the classified material is releasable.

(3) The Deputy Chief of Staff Intelligence (DCSINT) is the Foreign Disclosure Officer (FDO) for HQFM. United States owned classified material will not be disclosed to foreign nationals unless the release is coordinated with the Foreign Disclosure Office, Security Directorate, DCSINT with justification to support the disclosure.”

b. The Security Division, DPTMS, will maintain records on security clearances for personnel assigned to HQFM.

c. Security managers are the points of contact for receipt of security clearance data on visitors to their units/activities who require access to classified material to conduct official business.

d. Security Managers utilize JPAS to verify type of investigation, investigation date and date clearance is granted for official visit requests.

e. Security Managers utilize JPAS to verify investigative/clearance information for personnel who require access to IT Networks.

f. Documents generated by HQFM that are classified by “multiple sources” must include a listing of the sources when submitted for foreign disclosure approval.”

6-2. Nondisclosure Agreement

After subparagraph 6-2b, add the following:

“c. Security managers will administer the SF 312 briefing to personnel requiring access to classified material. Security managers will maintain a copy of the SF 312 video and briefing script provided by the Security Division, DPTMS.”

6-5. Debriefing and termination of classified access

Add the following sentences to the end of paragraph 6-5c:

“Cleared military and civilian personnel transferring to another DA command or federal agency will out-process through their Security manager. Out-processing will minimally include the following:

After subparagraph 6-5c, add the following:

(1) A briefing regarding the individual’s continued responsibility to protect classified material.

(2) Verification that classified and other accountable material possessed by the individual has been properly accounted for.

(3) Combinations and passwords previously issued to the individual have been changed.

6-10. Care during working hours

Add the following sentence to the end paragraph 6-10a:

“A sufficient amount of classified document cover sheets (SF 704 and 705) will be kept on hand to meet operational needs.”

Add the following sentences to the end of paragraph 6-10b(4):

“Make all notations on the SF 702 with non-erasable black ink. The SF 702 will be completed each duty day and may not be predated.

After subparagraph 6-10d(2), add the following:

“(3) Do not lock the container.”

After subparagraph 6-10e(3), add the following:

“f. To ensure a security container is locked, rotate the combination dial in a counter-clockwise direction at least four times; then, with the control drawer handle held in a depressed position, attempt to open each drawer of the container.”

6-11. End-of-Day security checks

Add the following sentence to end of subparagraph 6-11a:

“Retain the SF 701 and SF 702 at least 72 hours following the last entry or longer if needed as evidence in an investigation involving the compromise or possible compromise of classified material. Make entries on both forms with black (non-erasable) ink.”

After subparagraph 6-11b, add the following:

“c. End-of-day security checks will also include the checks of all classified magnetic media and electronic processing devices (i.e. electronic memory typewriters, facsimile machines, printers) used to process classified information to ensure classified material has been cleared, removed, destroyed, or stored in an approved security container.

d. List STU III/STE telephone keys/cards on the SF 701 as a part of end-of-day checks to ensure they have been removed from the phones at the end of each day.”

6-12. Emergency planning

Add the following sentences to the end of paragraph 6-12:

“Post the plan conspicuously near each security container. To serve a group of containers, post the plan in an area in the vicinity of all the containers. The emergency plan will include procedures for rooms that are alarmed in the event of a power outage. See Appendix J for a sample emergency plan.”

6-13. Telephone conversations

Add the following sentence to the end of subparagraph 6-13b:

“The MACOM/NERO is the proponent for issuing policy regarding the installation and operation of STU III/STEs in personal residences.”

6-14. Speakerphone guidance

After subparagraph 6-14e, add the following:

“f. Report mishaps involving possible security compromises or violations to the CSM immediately.”

g. Within HQFM, speakerphones will not be used for classified conversations without the approval of the CSM. Approval will be strictly limited and granted on a case-by-case basis.”

6-16. Visits

After subparagraph 6-16c, add the following:

“d. Visitors to HQFM will have their security manager forward a security clearance verification letter to the security manger of the unit/activity being visited, prior to the visit.

(1) HQFM personnel traveling to another installation will have their security manager forward a security clearance verification letter to the security manager of the activity being visited.

(2) The Security Division, DPTMS, will attempt to verify the security clearance of individuals visiting HQFM without prior written notification via JPAS. Until verification is made, these visitors will not be granted access to classified material.

(3) DoD contractor personnel visiting will have their Facility Security Officer (FSO) provide a visit request to the Security Division, DPTMS, prior to any visit that will involve access to classified material. Visit requests will provide the following:

(a) Name of contractor.

(b) Social security number.

(c) Security clearance.

(d) Dates of visit.

(e) Purpose of visit.

(f) POC at HQFM.

(g) Name and telephone number of the FSO.

e. Security managers with a classified contract will maintain a current visit request on file for all contractor personnel. Forward a copy to the Security Division, DPTMS.

f. The security SOP will include procedures, if applicable, for the release or disclosure of material to foreign visitors

and clearance verification procedures for non-foreign visitors requiring access to classified material."

6-18. Classified meetings and conferences

Add the following sentences to the end of subparagraph 6-18a(1):

"In-house classified meetings will be held in designated areas approved by the CSM. Security managers will have an SOP approved by the CSM for each facility. A copy of the CSM approval memorandum and facility SOP will be maintained at each site. After the initial approval, any changes to the physical layout of the site or changes to the SOP must be approved by the CSM. When an approved site is not available, the CSM must approve the use of an uncleared facility.

Add the following sentences to the end of subparagraph 6-18b(10):

"The use of cellular phones, Blackberry's, pagers, and other unauthorized electronic devices is prohibited while attending classified meetings, sessions, and conferences. These devices will be turned off prior to entry."

6-19. Information processing equipment

After paragraph 6-19, add the following:

"a. Security managers will identify all equipment used to process classified information. Identification will include:

(1) Overall level of classified information processed.

(2) Procedures for safeguarding the equipment while classified information is processed or retained in the equipment.

b. The CSM will approve the use of fax machines to transmit or receive classified material up to and including SECRET. All other fax machines within HQFM WILL NOT BE USED TO PROCESS CLASSIFIED MATERIAL unless prior approval by the CSM."

6-20. Receipt of classified material

Add the following sentences to the end of paragraph 6-20:

“All official mail, to include Official First Class Mail, as defined in the DoD Postal Manual, has the potential for containing classified material. Procedures will be established to ensure the adequate physical protection of official mail, until a determination can be made as to whether the mail contains classified material. The following additional guidance is provided:

After paragraph 6-20, add the following:

“a. Physical security requirements apply only to official mail that is addressed to official government activities, and not individuals.

b. Within HQFM, only mail handlers that have a validated security clearance, and whose name appears on the installation access roster may accept registered or Official First Class Mail. It will be assumed that this mail contains classified material.

c. The security SOP will include procedures for protecting incoming mail, i.e., official first class mail marked “POSTMASTER RETURN SERVICE REQUESTED.” Newly appointed mail handlers with authorization to handle registered mail will be briefed on the protection of registered mail items. All mail handlers will be briefed on the handling of Official First Class mail that bears the statement “POSTMASTER Return Service Requested.” It will be assumed that this mail contains classified material. All briefings will be documented and a copy maintained on file with the security manager.”

d. Personnel assigned to the Directorate of Human Resources (DHR) (Military) Classified Mail Room, will acknowledge receipt of all classified documents that are received from another command (off post or a tenant activity), and return the receipt to the sender. Further receipting is not required.

e. Security managers will include in the security SOP procedures in the event classified material is inadvertently received.”

6-21. TOP SECRET information

Add the following sentences after the second sentence in subparagraph 6-21a:

“Commands will appoint a primary and alternate Top Secret Control Officer (TSCO) in writing and furnish a copy to the CSM. Within HQFM the TSCO is located at the DHR Classified Mailroom. The TSCO is not authorized at lower levels.”

Add the following sentence to the end of subparagraph 6-21b:

“TOP SECRET accountability registers, records, and receipt forms will also include the total number of pages in documents marked TOP SECRET.”

Add the following sentence to the end of subparagraph 6-21c:

“An annual 100 percent inventory of TOP SECRET material on hand will be completed no later than 31 December of each year. This annual requirement may also be met by conducting monthly inventories of 10 percent of TOP SECRET material on hand, as long as 100 percent reconciliation is accomplished by 3l December. Methods and results of inventories will be documented and retained on file, and available for review during annual inspections.”

Add the following sentence to the end of subparagraph 6-21f:

“A TOP SECRET disclosure record (DA Form 969) will be used to record the authorized disclosure of TOP SECRET material.”

6-22. SECRET and CONFIDENTIAL information

Add the following sentence to the end of paragraph 6-22:

“Each activity within HQFM that stores classified information will establish written procedures for controlling the material.”

6-23. NATO and Foreign Government material

Add the following sentence to the end of paragraph 6-23:

“All classified NATO access and documents will be controlled and stored by the NATO Control Officer, DCSINT. Requests for temporary storage of NATO documents elsewhere must be in writing and submitted to the DCSINT for approval.”

6-24. Working papers

Add the following sentence to the end of subparagraph 6-24a(2):

“All markings will be in non-erasable black ink.”

Add the following sentence to the end of subparagraph 6-24a(6)(b)

“Working papers will be maintained for no more than 180 days.”

6-26. Approval for reproduction

Add the following sentences after the first sentence in subparagraph 6-26a:

“All copiers used for the reproduction of classified material will be approved in writing by the CSM. An SOP, approved by the CSM, will be posted on or near each approved copier. The SOP will list, at least by position, those persons authorized to approve classified reproduction, the highest classification level of material that may be reproduced, and procedures in the event of a power failure or equipment malfunction. Approved copiers for classified reproduction will be re-validated if there is any change to the copier, i.e., copier moved to a different location.”

After subparagraph 6-26c, add the following:

“d. “The CSM is the TOP SECRET reproduction control official for HQFM. The HQFM TSCO is the only individual authorized to reproduce TOP SECRET information upon written authorization by the CSM. The NATO Control Officer is the only individual authorized to reproduce NATO classified information upon written authorization by the DCSINT.”

6-27. Policy

After subparagraph 6-27a, add the following:

“(1) Classified material will be properly destroyed when no longer required for mission accomplishment or, if law or regulation no longer requires retention.

(2) The CSM will approve, in writing, all classified destruction devices, i.e., shredders, prior to use. Coordinate with the Security Division, DPTMS, prior to purchasing any equipment for classified destruction.

(3) Personnel who destroy classified material will have a valid security clearance and be listed on the installation access

roster. Classified material hand carried from one building to another for destruction requires the individual to have a current DD Form 2501, Courier Authorization, in their possession.

6-36. Entry Exit Inspection Program and Two Person Integrity for TOP SECRET Information

Add the following sentences to the end of paragraph 6-36:

“Within HQFM, the Two Person Integrity Program is required. The unauthorized disclosure of TOP SECRET information can result in exceptionally grave damage to national security. Employees will not be permitted to work alone in areas where TOP SECRET classified material is in use. When compelling operational requirements indicate the need, the CSM may waive this requirement.”

7-1. Policy

Add the following sentences to the end of paragraph 7-1:

“Security containers used to store classified material will not be used to store “unrelated” unclassified material. Classified and “related” unclassified material may be stored in the same container. Arms, ammunition and explosives (AA&E) (including arms room keys) will not be stored in containers used to store classified material. Classified equipment may be stored in security containers with classified documents. Classified weapons and/or ammunition must be stored in an arms room authorized to store classified material.”

7-4. Storage of classified information

Add as the first sentence to subparagraph 7-4a:

“The storage of TOP SECRET information within HQFM is authorized only at the DHR(Mil) Classified Mail Room.”

Add the following sentences to the end of subparagraph 7-4b(1):

“On a case-by-case basis, units may use GSA approved field safes and one-drawer security containers for the storage of classified material while in a field environment, however, safes will be secured to a solid permanent fixture by a chain and padlock. These provisions apply only to the storage of SECRET and CONFIDENTIAL material.”

After subparagraph 7-4b(3), add the following:

“(4) Within HQFM, steel filing cabinets, with or without lock bars, are not authorized for the storage of classified material.”

7-6. Residential storage

After subparagraph 7-6c, add the following:

“d. The MACOM/NERO is the proponent for issuing policy regarding the installation and operation of secure telephone units in personal residences.

e. The storage of SECRET and CONFIDENTIAL material in personal residences, either on or off a military installation, requires the approval of the MACOM/NERO. Requests will be submitted through the CSM to the MACOM/NERO. Requests will be fully justified and contain assurances that all classified storage requirements are met.” An inspection will be conducted by the Security Division, DPTMS prior to approval of the request.”

7-8. Equipment Designations and Combinations

Add the following sentences to the end of subparagraph 7-8a:

“Security managers will maintain a master list with the identification number and location of each security container. Security containers will be numbered consecutively. No two containers in an activity will have the same number. Record the container number on the SF 700. Activities with more than one security container will designate a master container to hold combinations to the other containers. The master container shall be identified as Container #1. If an activity has only one security container, it shall be identified as Container #1. The combination to safe #1 will be stored on SF Form 700, Part B, at the DHR(Mil) Classified Mail Section.”

Add the following sentences after the first sentence of subparagraph 7-8b:

“Within HQFM call the Service Order Desk, Directorate of Public Works (DPW) at 788-4228 to request a combination change to a GSA approved security container. The locksmith may prepare the lock for a combination change and teach the Security Manager/ authorized person the procedure for changing the combination. The new combination will only be set by the security manager/

authorized person. The locksmith will not have access to the combination under any circumstance. The security manager/authorized person will test the new combination at least three times before locking the container while the locksmith is still present."

After subparagraph 7-8b(6), add the following:

"(7) Combinations will be changed no later than 24 hours following the occurrence of situations identified in paragraph 7-8b (1 through 5) of AR 380-5. All individuals with knowledge of safe combinations will be listed on the activity/unit access roster."

Add the following sentence after the first sentence of subparagraph 7-8c:

"All security containers not authorized for classified storage will have a notation affixed to the front of it as follows: NOT AUTHORIZED FOR STORAGE OF CLASSIFIED INFORMATION."

Add the following sentence to the end of subparagraph 7-8c(1):

"All entries on SF 700 will be typed or written in non-erasable black ink."

Add the following sentence after the second sentence of subparagraph 7-8C(4):

"For all security containers within an activity (except Container #1), secure Parts 2 and 2A of the SF 700 in Container #1. Parts 2 and 2A of SF 700 to Container #1 will be hand carried to the Classified Mail Section DHR, and secured, before close of business the day the combination is changed. Commanders of tenant units/activities will include procedures in their Security SOP on how classified container combinations will be filed and safeguarded within their areas."

Add the following sentence to the end of subparagraph 7-8f:

"No two containers within the same unit, activity, or office will have the same combination."

After subparagraph 7-8f, add the following:

“g. Memory/convenience “keys”, such as birthdays, telephone numbers, street addresses, or social security numbers, will not be used as combinations.”

h. A combination (SF 700, Part 2A) subject to investigation due to compromise or possible compromise of classified material will not be destroyed until approved by the CSM.”

7-9. Repair of Damaged Security Containers

Add the following sentences to the end of paragraph 7-9:

“If a security container cannot be opened (a lockout has occurred); report it immediately to the Security Division, DPTMS. A lockout occurs when a security container malfunctions, i.e., will not open or close due to normal wear and tear, negligence, or tampering. Once the CSM confirms the malfunction, the security manager will call the DPW Service Order Desk at 788-4228 and submit a work order request. The activity/unit security SOP will include procedures for handling security container and secure room lockouts.”

7-11. Turn-in or Transfer of Security Equipment

Add the following sentences to the end of paragraph 7-11:

“The activity security manager will affix a signed statement to the front of the container, which says that it does not contain classified material. The SF 700 is not required when the safe combination has been reset to the standard combination 50-25-50. To have a combination reset, contact the DPW Service Order Desk.”

7-12. General

Add the following sentences to the end of paragraph 7-12:

“New construction and upgrades to existing facilities involving the open storage of classified equipment or the certification of classified meeting sites will be coordinated, in advance, with the CSM. The CSM will ensure that all applicable security requirements are incorporated into the initial planning.”

After paragraph 7-12, add the following:

“a. Open storage of classified material will be kept to a minimum, and only approved when necessary for mission

accomplishment or when the volume or size of the classified material prohibits storage in a GSA-approved security container.

b. The CSM is the approving authority for open storage areas within HQFM. Approvals will be in writing, and will be granted only after the open storage area has been inspected and certified by the CSM. Additionally, an SOP for open storage of classified material must be submitted to the CSM for review and approval.

c. A copy of the approval and SOP will be maintained on file within the open storage area. The original approval documentation will be maintained on file by the security manager and available for review during inspections.

d. Open storage approvals are valid for up to 5 years. Approvals will be re-issued after the facility has been inspected and re-certified by the CSM. Open storage approvals will be terminated when structural modifications that degrade security are made.”

7-13. Vault and Secure Room (Open Storage Area) Construction Standards

After subparagraph 7-13b(5), add the following:

“c. Whenever feasible, to provide maximum level of protection, newly constructed open storage areas will meet the more stringent construction standards of a vault.

d. The open storage standards and requirements identified in Chapter 7 and this supplement are only minimum standards, and whenever possible, should be augmented with supplementary controls to provide maximum protection of the classified material.

(1) Cover classified material that is openly displayed in secure areas (i.e. maps, charts, etc.), to prevent observation by visitors who do not have a need-to-know.”

7-20. Minimum standards for deviations to construction standards for open storage areas

After subparagraph 7-20e, add the following:

“f. Requests for deviations to construction standards for open storage areas will be fully justified, and will include proposed

compensatory systems, controls, or procedures to properly protect the classified material and sufficiently deter, detect delay, or deny unauthorized penetration into the secured area. Request for deviations to construction standards for open storage areas will be submitted, in writing, to the MACOM/NERO through the CSM.

(1) Approvals for deviations to construction standards will be in writing, and will be granted only after the open storage area is inspected and certified to meet the minimum requirements and standards, or after approved compensatory measures are in place.

(2) A copy of the deviation approval documentation will be maintained on file within the open storage area. The Security Division, DPTMS, will also maintain a copy."

8-1. Policy

After paragraph 8-1, add the following:

"a. Protect classified documents hand carried between buildings on a government facility by placing them in a sealed opaque envelope. A locking briefcase may serve as the outer wrapper. Stamp the envelope top and bottom, front and back, with the highest classification of its contents. In case of loss, address the envelope with the organization address of the individual hand carrying the material (return and forwarding address are the same).

b. The SF 65, US Government Message Envelope, will not be used for internal routing or transporting of classified material. Before releasing classified material to another person, ensure the recipient has the appropriate security clearance. The courier will be advised that the package contains classified material. The activity/unit security SOP will include procedures for mailing classified material. The SOP will also include procedures for protecting incoming official First Class Mail."

c. Classified material (SECRET and CONFIDENTIAL) for dispatch from Fort Monroe through the US Postal Service (USPS) by Registered Mail (SECRET) or First Class Mail (CONFIDENTIAL, only), will be hand carried to the DHR(Mil) Classified Mailroom, for processing.

d. Coordinate shipments of bulk or oversized classified material or equipment that exceeds the size limitations of the

USPS, with the DPW, Supply and Services Division, Property Book Branch.

e. The CSM will approve, in writing, the use of facsimile machines to transmit or receive classified material up to and including SECRET.

f. The activity/unit security SOP will include procedures for mailing classified material and protecting incoming mail, i.e., official first class mail marked “POSTMASTER RETURN SERVICE REQUESTED.”

8-3. SECRET Information

Add the following sentence to the end of subparagraph 8-3f:

“Within HQFM, only the USPS express mail is authorized for next-day delivery service.”

8-4. Confidential information

Add the following sentence to the end of subparagraph 8-4c:

“As a minimum, first class mail bearing the above caveat will be protected as classified material until it can be determined if it contains classified information.”

8-9. Envelopes or containers

Add the following sentence to the end of subparagraph 8-9a(5):

“Within HQFM, a locked briefcase may serve as the outer wrapper for classified material hand carried on Fort Monroe and within the 75 mile geographical limit.”

8-12. General provisions

After subparagraph 8-12b, add the following:

“c. Within HQFM, two persons with local TOP SECRET access are required to hand carry TOP SECRET material.

d. The hand carry of TOP SECRET material is limited to individuals approved in writing by the CSM.

e. Refer to Appendix K of this supplement for specific procedures on the hand carry of classified material.”

8-13. Documentation

Add the following sentence to the end of subparagraph 8-13b:

“Within HQFM , the DD Form 2501, Courier Authorization Card, will only be used to identify appropriately cleared DoD personnel (including contractors) authorized to hand carry classified material, locally (within 75 miles).”

Add the following sentences to the end of subparagraph 8-13b(2):

“Within HQFM, the security manager will sign the DD Form 2501 as the authorizing official. If the security manager has a requirement to locally hand carry classified material, the alternate security manager or the individual’s unit or activity head will sign the DD Form 2501 as the authorizing official.”

Add the following sentences to the end of subparagraph 8-13b(3):

“DD Form 2501 (blank) will be stored in a GSA-approved container. Forms will be accounted for at all times. Security managers will report the loss or inadvertent destruction of a blank DD Form 2501 to the CSM immediately.”

Add the following sentence to the end of subparagraph 8-13b(4):

“Within HQFM, the DD Form 2501 will be issued in 1 year increments.”

After subparagraph 8-13b(5), add the following:

“c. Security managers shall request a bulk issue of blank DD Forms 2501 from the DHR Publications Stockroom, Building 28, Fort Monroe. Quantities shall not exceed a reasonable amount for mission accomplishment. Unit/activity commanders shall submit DD Form 577 (Signature Card) to the Publications Stockroom Manager. The use of DD Form 577 authorizes the security manager to sign for DD Forms 2501. Forms will not be issued if a signature card is not on file.

After subparagraph 8-13c, add the following:

“(1) Documentation of courier briefings will be maintained by the unit/activity for 2 years following departure, transfer, or separation of the designated courier.”

(2) The record of issue will be maintained by the unit/activity

for 2 years following the last entry on the record. See Figure K-6 for a sample record of issue."

(3) Copies of the DA Form 410 (Receipt for Accountable Forms) will be maintained by the unit/activity for 2 years after the last DD Form 2501 in the series has been issued."

8-14. Security requirements for temporary duty travel outside the United States

Add the following sentences to the end of subparagraph 8-14a:

"Requests to hand carry classified material for foreign disclosure will be coordinated in advance with the DCSINT Foreign Disclosure Office."

After subparagraph 8-14f, add the following:

"g. Hand carry of classified material to OCONUS locations will only be conducted when no other acceptable method is available. More secure means will be used whenever possible.

h. Classified material that requires additional controls or handling procedures (NATO, COMSEC, etc.) will be hand carried in accordance with applicable governing regulations."

8-15. Hand carrying or escorting classified material aboard commercial passenger aircraft

After subparagraph 8-15b, add the following:

"c. The provisions of paragraph 8-14, and this supplement, apply to the hand carry of classified material aboard commercial aircraft."

d. Refer to Appendix K for additional procedures."

9-1. General Policy

Add the following sentences after the second sentence of paragraph 9-1:

"Commanders and activity heads will implement a security education program to ensure their personnel are continuously informed of security policies and procedures. The CSM is responsible for providing guidance, technical advice, and assistance to commanders and security managers on what security

requirements, at minimum, will be implemented. Procedures for reporting security violations will be incorporated into the activity/unit security SOP."

9-2. Methodology

Add the following sentences after the second sentence of paragraph 9-2:

"Initially, and annually thereafter, security managers will provide a security briefing based on paragraph 9-4, to all personnel. Special emphasis will be given to personnel with access to classified material. Briefings will be documented and maintained on file with the security manager. Initial and refresher security training is the responsibility of the security manager of the individual's "duty" location. Example: A soldier is assigned to HQFM with duty at the United States Army School of Music. The School security manager is responsible for initial and refresher training for that soldier as long as his/her duty location is at the School."

9-3. Initial Orientation

Add the following sentences after the first sentence of paragraph 9-3:

"The security education program will include an initial security orientation for all new personnel within 30 days of assignment. The initial orientation will cover, at minimum the requirements of AR 380-5, paragraph 9-4. Security managers will maintain briefing certificates or attendance rosters on file for review during inspections."

9-7. Refresher Briefing

Add the following sentences to the end of paragraph 9-7:

"Annual refresher briefings will cover, at a minimum, the requirements of paragraph 9-4 and the unit/activity security SOP. Security managers will maintain briefing certificates or attendance rosters on file for review during inspections."

9-8. Foreign travel briefing

After subparagraph 9-8d, add the following:

“e. DA Military and civilian personnel scheduled to travel outside the US and its territories or possessions (PCS, TDY, leave/vacation) will contact their security manager prior to travel to schedule a Foreign Travel Briefing (Level I Antiterrorism/Force Protection briefing) prior to departure. The security manager will contact the DPTMS Antiterrorism/Force Protection Officer to arrange for a briefing. Units/activities with trained and certified Force Protection Unit Advisors will conduct the training. Procedures for coordinating or conducting foreign travel and Level I Antiterrorism/Force Protection awareness briefings will be incorporated into the unit/activity security SOP.”

9-14. Others

After subparagraph 9-14f, add the following:

“g. Procedures for coordinating or conducting SAEDA training will be incorporated into the activity/unit security SOP.”

9-15. General Policy

Add the following sentences after the first sentence of paragraph 9-15:

“Security managers, or their designee, will conduct termination briefings for unit/activity personnel. Termination briefings are required for individuals upon retirement, reassignment, ETS, or when no longer required to have access to classified material. The individual being briefed will complete an original of the DA Form 2962, Security Termination Statement and Debriefing Certificate or the SF 312, Non Disclosure Agreement. Security managers will maintain the completed DA Form 2962 or SF 312 on file for 2 years. See 380-5, paragraph 6-5, Debriefing and Termination of Classified Access.”

9-16. General Policy

Add the following sentence after the first sentence of paragraph 9-16:

“The CSM will evaluate the effectiveness of security education programs during command inspections.”

10-1. General policy

After subparagraph 10-1d, add the following:

“e. The CSM will immediately initiate the preliminary inquiry (PI) process upon learning of a possible loss or compromise of classified information.”

10-2. Reaction to discovery of incident

Add the following sentences to the end of subparagraph 10-2b:

“Within HQFM, any person who becomes aware of the possible compromise of classified information during regular duty hours will immediately notify the DPTMS Security Division at 788-2851. During non-duty hours, notify the TRADOC IOC Staff Duty Officer, Bldg 267 at 788-6304 or 277-8278.

10-3. The preliminary inquiry

Add the following sentence after the second sentence of paragraph 10-3:

“Within HQFM, the CSM will notify the unit/activity commander, in writing, to initiate the PI.”

Add the following sentences to the end of subparagraph 10-3a:

“Upon written notification from the CSM to initiate a PI, the unit/activity commander will appoint, in writing, a person (hereafter, referred to as investigating officer) to conduct the PI by the conclusion of the next duty day. Refer to Appendix L, for guidance on conducting a PI and to Figure L-1 for a sample appointment memorandum.”

After subparagraph 10-3c(3), add the following:

“(4) “Results of PIs will be prepared in the format provided at Figure 10-1, AR 380-5. PI reports will be unclassified whenever possible. However, if it is absolutely necessary, they will be classified at the highest level of the information contained therein. PI reports will contain appropriate classification authority and declassification instructions. Classified PI reports will be appropriately safeguarded, stored and controlled.”

Add the following sentences to the end of subparagraph 10-3f:

“The investigating officer will notify the CSM and his/her chain of command if at any time during the PI it appears that deliberate compromise of classified information may have occurred. The CSM will notify the Fort Monroe Resident Office, 902d Military Intelligence (MI) Group. The PI will stop until the 902d MI Group can conduct an investigation. At the conclusion of the MI investigation, the CSM will notify the investigating officer and their unit/activity commander to complete the PI.”

After subparagraph 10-3f, add the following:

“g. The investigating officer will submit the results of the PI to the unit/activity commander within 10 workdays from the date of appointment. The CSM may grant an extension to the deadline based on extenuating circumstances.

h. Within 3 days of receipt, the unit/activity commander will forward the completed PI report with cover memorandum, through command channels, to the CSM. The memorandum will, either concur or non-concur with the findings and recommendations of the investigating officer, outline proposed corrective actions and determine if an additional investigation is warranted (i.e. AR 15-6. Refer to Figure L-2 for a sample cover memorandum).

i. The CSM will ensure PIs are promptly and properly completed, and the results reported to the proper authorities.”

10-4. Reporting results of the preliminary inquiry

Add the following sentence after the first sentence of subparagraph 10-4a:

“The CSM will notify the OCA.”

After subparagraph 10-4e, add the following:

“f. The CSM will review the completed PI report with cover memorandum, and determine if the findings, and corrective actions are sufficient to resolve and close the PI, or if other actions are warranted, as specified in paragraph 10-4.”

10-5. Reevaluation and damage assessment

Add the following sentence to the end of subparagraph 10-5a: “The CSM will assist the OCA in preparing a damage assessment, if required.”

10-7. Management and oversight

After subparagraph 10-7a, add the following:

“(1) Security incidents involving minor violations of established security regulations in which no compromise has occurred, may be considered an administrative discrepancy, as determined by the CSM, and may not require a PI.

(2) Administrative discrepancies would normally not require any remedial, administrative, or disciplinary action; however the CSM will make that determination. If negligence is involved, or if the possibility of compromise or damage to national security exists, the violation will not be considered an administrative discrepancy.”

10-8. Additional Investigation

After paragraph 10-8, add the following:

“a. Additional AR 15-6 investigations should only be conducted for the purposes identified in this paragraph, or when the CSM, unit/activity commander or higher headquarters determines that the investigation would be productive in providing further clarification of the causes and responsibility for a compromise or security violation. Investigations will be conducted in strict accordance with the provisions of AR 15-6 and command policy.

b. Corrective actions identified by the PI, notification of originators, and reporting requirements will not be delayed pending the results of AR 15-6 investigations.

c. Appointed investigating officers will obtain a legal review of the completed AR 15-6 investigation report before submitting to the appointing authority. The appointing authority will provide a copy of the finalized report to the CSM for review and appropriate action.”

10-9. Unauthorized absences, suicides, or incapacitation

After paragraph 10-9, add the following:

“a. Any incident described in this paragraph which involves DA military or civilian personnel who have had access to classified information, will be immediately reported to the CSM to determine if further investigation or action is required.”

b. If required, a PI will be conducted.”

//*S//
JASON T.EVANS
Colonel, Adjutant General
Commanding

Distribution:
fort.monroe.army.mil

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

***Original signed document on file in the Publications Control Office, Fort Monroe**

Appendix A
References

Section V
Mandatory References for Security Managers

AR 25-2, Information Assurance.

AR 380-5, Department of the Army Information Security Program.

AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives.

AR 380-67, The Department of the Army Personnel Security Program.

AR 381-10, US Army Intelligence Activities.

AR 381-12, Subversion and Espionage Directed Against the US Army (SAEDA).

AR 525-13, Antiterrorism.

AR 530-1, Operations Security (OPSEC).

HQFM Security Initial/Refresher Training (Cleared Persons) Power Point Presentation.

HQFM Security Initial/Refresher Training (Uncleared Persons) Power Point Presentation.

Guide to marking classified documents as modified by the Information Security Oversight Office (ISOO) implementing directive number 1, “Classified National Security Information;” 22 Sep 03.

Standing Operating Procedure (SOP) for Personnel Security Managers, DPTMS Security Division, 23 Nov 05.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Appendix J
Sample Emergency Plan for the Protection of Classified Material

J-1. Reference. Paragraph 6-12, AR 380-5, Department of the Army Information Security Program.

J-2. Purpose. To establish procedure and assign responsibilities for the protection of classified material in the event of an emergency.

J-3. Responsibilities.

a. The unit/activity commander or designated representative is responsible for implementing the procedures within this plan.

b. All personnel listed on the SF 700 will be knowledgeable of this plan and be able to execute it, when necessary.

J-4. Implementation. This plan will be implemented on the order of the unit/activity commander; his/her designated representative, the Garrison Security Manager or the Garrison Commander.

J-5. General procedures. Security managers will continuously review classified holdings to ensure that only classified material needed for mission accomplishment is retained.

a. Civil disturbances. Secure classified material in appropriate security containers and post knowledgeable individuals at each entrance to control access to the facility. If the seriousness of the situation warrants, the Garrison Commander will direct military police to provide security.

b. Fire. To ensure that risk of injury or loss of life is minimized, the following actions will be taken:

(1) Leave classified material in place.

(2) Do not take time to secure classified containers.

(3) Position personnel around the sensitive area to prevent the unauthorized removal of classified material.

d. Natural disaster. When flooding is expected, move classified material and equipment to a location to ensure their protection. Disconnect all electrical equipment from electrical outlets and, if possible, place the equipment above floor level.

e. Enemy action. Unless otherwise directed, or when emergency removal is impractical due to the volume of classified material, personnel will ensure classified material is secured in GSA-approved containers and those entrances into the area are secure. Total destruction of classified material will occur only at the direction of the Garrison Commander.

f. In situations not specifically anticipated by this plan, or when circumstances warrant, the senior person present may deviate from the procedures in this plan.

g. A copy of this plan will be posted on or near each container or group of containers used to secure classified material.

Appendix K
Hand carry of Classified Material

K-1. Purpose. To establish procedures for the hand carry of classified material by personnel assigned to HQFM to include tenants.

K-2. General.

a. Classified material may be hand carried when no other approved means are available. Approved means include the United States Postal Service (USPS), classified facsimile, or electronic mail via the Secure Internet Protocol Routing Network (SIPRNET).

b. Appropriately cleared couriers may hand carry classified material up to SECRET locally (within a 75 mile radius of Fort Monroe) if authorized by the unit/activity security manager.

c. The hand carry of classified material within the Continental United States (CONUS) beyond the 75-mile limit must be approved, in writing by the CSM.

d. The hand carry of classified material Outside the Continental United States (OCONUS) aboard commercial aircraft must be approved by the MACOM/NERO.

e. Couriers of TOP SECRET material must be approved by the (CSM), in writing, and will be issued a DD Form 2501, specifically for the hand carry of TOP SECRET material.

f. Within HQFM, two person integrity is required to hand-carry

TOP SECRET material within the local 75-mile limit .

g. All couriers will receive a one-time courier briefing and will sign a briefing statement (Figure K-2) acknowledging the briefing prior to being issued a DD Form 2501. The security manager will maintain the briefing statement on file for review during annual inspections.

h. Courier authorization is not required in the event of a unit deployment on military aircraft or military chartered aircraft.

i. The security manager will advise the CSM if classified material is destined for use strictly by the US government or if foreign disclosure is possible. If information is for foreign disclosure, it must be approved in accordance with AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, prior to disclosure.

K-3 Procedures.

a. Local Hand carry. The security manager will issue a DD Form 2501 to all individuals authorized to hand carry classified information locally. DD Form 2501 must be in the possession of the courier while transporting classified material. Prior to issuing a courier card, the security manager will brief the courier (see Figure K-1) on his/her responsibilities. The courier will acknowledge receipt of the briefing by signing a courier briefing statement (see Figure K-2). A DA Form 3964 (Classified Document Accountability Record) or DA Form 455 (Mail and Document Register) is required when hand carrying classified material to DoD contractors.

b. CONUS Hand carry. Security managers will submit a request to hand carry classified material within CONUS (beyond the 75 mile local limit) to the CSM for approval (Figure K-3). A completed DA Form 3964 or DA Form 455 listing the material being hand carried must accompany the request. Prior to the courier mission, the courier will receive a briefing from the security manager (see Figure K-4). The security manager will document the briefing (see Figure K-2) and maintain a copy on file. Individuals that frequently conduct off-post courier missions may be briefed at 6-month intervals; however, this is in addition to the one-time briefing required when an individual is first issued a DD Form 2501.

(1) The security manager will make arrangements, in advance,

for the proper storage of the classified material at TDY locations and at all stops in route. Classified material may only be stored at a US Government facility, or a cleared DOD contractor facility with approved storage capability.

(2) The Security Division, DPTMS, will issue a courier authorization letter to the individual designated to conduct the courier mission. The Security Division, DPTMS, will retain a copy of the letter with the completed DA Form 3964, or DA Form 455.

c. OCONUS Hand carry. The appropriate MACOM/NERO must approve all requests to hand carry classified material (up to SECRET) on commercial aircraft OCONUS.

(1) The security manager will submit a completed OCONUS Hand carry Request Form (Figure K-5) to the CSM with a completed DA Form 3964 or DA Form 455, for approval.

(2) If all items on the form are marked GO, the CSM will recommend to MACOM/NERO the approval of courier authorization. If authorization is granted, the CSM will issue the authorization memorandum, with a control number, immediately following the mission destination.

(3) The original memorandum will be given to the individual; one copy will be retained by the Security Division, DPTMS, along with the DA Form 3964, or DA Form 455.

(4) Prior to an OCONUS mission, the designated courier will be briefed by the activity security manager (Figure K-4) who will document the briefing with a signed statement (Figure K-2). The security manager will maintain the briefing statement on file. Individuals who frequently conduct courier missions OCONUS may be briefed at 6-month intervals. This briefing requirement is in addition to the one-time briefing required when an individual is first issued a Courier Authorization Card.

(5) If the completed OCONUS Hand carry Request Form included NO GO responses, courier authorization will not be granted by the CSM. If a NO GO situation cannot be resolved, and the mission is still valid, the CSM will contact the MACOM/NERO for assistance, e.g., resolve the NO GO issue(s), grant an exception to policy, or make a final disapproval of the request.

d. General Instructions. As a designated courier of classified material, you are authorized to hand carry or escort

material on this installation, plus 75 miles. In some situations, you may not have actual access or specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become the custodian of that information as defined in AR 380-5.

e. Responsibility. All military personnel and DA civilian employees are subject to Title 18, United States Code (USC) concerning the unauthorized release of national security information. However, as a courier, you are solely and legally responsible for protection of the material in your possession. Your responsibility lasts from the time you receive the material until it is delivered to the station, agency, unit, or activity listed as the official addressee.

f. Intent. The intent of this briefing is to familiarize you with your responsibilities as a courier, duties as a custodian, and the security and administrative procedures governing the safeguards and protection of classified material. You must become familiar with the provisions of AR 380-5, Department of the Army Information Security Program, and FM Supplement 1 to AR 380-5, with special emphasis on the following areas:

(1) Access. Dissemination of classified material is restricted to those persons who are properly cleared and have an official need for the information. No person has a right or is entitled to access of classified material solely by virtue of rank or position. To help prevent unauthorized access and possible compromise of material entrusted to you, it must be retained in your personal possession or properly guarded at all times. You will **NOT** read, study, display, or use classified material while in public places or conveyances.

(2) Storage. Whenever classified material is not under your personal control, it will be guarded or stored in a GSA-approved security container. You will **NOT** leave classified material unattended, i.e., in locked vehicles or car trunks.

(3) Preparation. Whenever you transport classified material, it must be enclosed in two opaque sealed envelopes, similar wrappings, or two opaque sealed containers such as boxes or other heavy wrappings. A locking briefcase may serve as an outer wrapper or container. The inner envelope or container will be addressed to the activity the individual belongs to (as if for mailing), stamped with the highest classification and placed inside the second envelope, container, or briefcase. The outer covering (with the exception of the briefcase), will be sealed

and addressed to the activity the individual belongs to. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission.

g. Hand carrying. The DD Form 2501, Courier Authorization Card, permits you to hand carry classified material on the installation to which you are assigned, plus 75 miles. The courier card must remain in your possession at all times when hand carrying classified material. If your courier card should become lost or stolen, you must report it immediately to your activity security manager, who will then notify Security Division, DPTMS. The DD Form 2501 is an accountable item. It will be returned to the security manager upon expiration or when no longer required, e.g., individual transfers, terminates their employment, or retires, whichever occurs first.

h. Conclusion. The primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations cannot guarantee protection of classified material nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information. If you have questions at any time concerning the security and protection of classified material entrusted to you, contact your security manager or the Security Division, DPTMS.

Figure K-1. Courier Briefing For Local Hand carry of Classified Material

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Sample Courier Briefing Statement

As a courier of classified material, I have received a briefing on the procedures for hand carrying Classified material and understand my responsibilities as a courier.

NAME:
_____

SSN:
_____

ACTIVITY:
_____

DATE:
_____

SIGNATURE:
_____

Figure K-2. Courier Briefing Statement

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Courier Authorization Memorandum

IMNE-MNR-PL Date

TO WHOM IT MAY CONCERN

SUBJECT: Courier Designation

1. In accordance with AR 380-5, Department of the Army Information Security Program, (insert traveler's name, SSN, and organization), who is employed or is a military member of the organization, is on official government business and designated as a courier to hand carry classified material in conjunction with travel indicated below. Material is double wrapped in a (insert size) envelope, addressed to: (insert address).

a. Departure point: _____.

b. Departure date: _____.

c. Destination(s): _____.

d. Known transfer point(s): _____.

e. Issue date: _____.

2. A listing of the transported material is on file at the Security Division, DPTMS, Fort Monroe, Va.

3. There is neither time nor alternate means of transmission available to send the material referred to herein that would provide for timely accomplishment of operational objectives. This letter may be confirmed by calling the undersigned at (757) 788-2851 or DSN 788-2851, during normal duty hours.

4. This letter of authorization expires _____. (Insert date not to exceed 7 days from date of issue, or in the event of a round trip, 7 days after scheduled date of return).

(Signature Block of CSM)

Figure K-3. Courier Authorization Memorandum (CONUS)
(Note: HQFM letterhead will be used)

Courier Briefing For CONUS/OCONUS Hand Carry of Classified Material

1-1. General Instructions. As a designated courier of classified material, you are authorized to hand carry or escort material while in a travel status between your duty and TDY stations. In some situations, you may not have actual access or specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become the custodian of that information.

2-1. Responsibility. All military personnel and DA civilian employees are subject to Title 18, United States Code, concerning the with unauthorized release of national security information; however, as a courier, you are solely and legally responsible for protection of the material in your possession. The responsibility lasts from the time you receive the classified material until the material is properly delivered to the station, agency, unit, or activity listed as the official addressee.

3-1. Intent. The intent of this briefing is to familiarize you with your responsibilities as a courier, the duties of a custodian, and the security and administrative procedures governing safeguarding and protecting classified information. You must be familiar with the provisions of AR 380-5, Department of the Army Information Security Program, and this supplement, with special emphasis on the following areas:

a. Access. You will be given delivery instructions for the material when it is released to you. Follow those specific instructions and seek assistance from a responsible official if you are unable to do so. Dissemination of classified material is restricted to those persons who are properly cleared and have an official need for the information. No person has a right or is entitled access to classified material solely by rank or position. To prevent unauthorized access and possible compromise of material entrusted to you, it must be retained in your personal possession or properly secured at all times. Do not read or display classified material while in public places or conveyances.

b. Storage. When classified material is not under your personal control, it will be guarded or stored in a GSA-approved security container. You will not leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, or storage compartments in the passenger section of

commercial airlines or when aboard trains, or buses. You will not store the material in detachable storage compartments such as trailers, luggage racks, or aircraft travel pods. You will not pack classified items in regular checked baggage. Retention of classified material in hotel/motel rooms, or personal residences, is strictly prohibited. Safety deposit boxes provided by hotels/motels do not provide adequate storage for classified material. An advance arrangement for proper overnight storage at a US Government facility or, if in the United States, a cleared contractor’s facility is required prior to departure. Arrangements are the responsibility of the unit/activity requesting the transmission of classified material.

c. Preparation. When you transport classified material, it must be enclosed in two opaque sealed envelopes, two opaque sealed containers such as boxes or other heavy wrappings without metal bindings or similar wrapping. A briefcase, when used, will not serve as an outer wrapping. The inner most envelope will be stamped with the highest classification (top and bottom, front and back), and addressed (as if for mailing) to the government activity. The outer most envelopes will be sealed and addressed for mailing (in event of emergency) to the government activity. Do not accept improperly prepared material for transmission. Receipts will be exchanged when and if required.

d. Hand carry. The written courier authorization memo should ordinarily permit you to pass through passenger control points within the US without the need to subject the classified material to inspection. Except for customs inspection, airports have established screening points to inspect all hand carried items. If you are hand carrying classified material in envelopes, you should process through the ticketing and boarding procedures in the same manner as other passengers. When sealed envelopes are carried in a briefcase (carry on luggage), the briefcase may be routinely offered for inspection for weapons. The screening official may check the envelope by x-ray machine, flexing, feel, weight, etc., without opening the envelope. If the screening official is not satisfied with your identification, courier authorization memo, or envelope, you will not be permitted to board the aircraft and are no longer subject to further screening. **Do not allow the screening official to open envelopes containing classified material as a condition for boarding the aircraft.**

e. Escorting. When escorting classified material that is sealed in a container and too bulky to hand carry, or is exempt from screening, prior coordination with the Federal Aviation

Authority (FAA) and the airline involved, is required. Coordination is the responsibility of the approving authority. Designated couriers will report to the airline ticket counter prior to starting the boarding process. If all requirements are met, the container will be exempt from screening. An airline official will escort the courier to the screening station and exempt the container from physical or other type inspection. If all requirements are not met you will not be permitted to board the aircraft with the container and no further screening will be done. Under no circumstance will airline officials be permitted to open the sealed container.

f. Loading and Unloading. The loading and unloading of bulky material will be under the supervision of a representative of the airline; however, the designated courier will accompany the material and keep it under constant surveillance during loading, until the hatch is secured. The designated courier will be the first to exit the plane at the destination and will be on the unloading platform when the hatch is opened to view the unloading process and to take possession of the material. Appropriately cleared personnel will be available to assist in surveillance at any intermediate stops and when the cargo compartments are opened. Coordination of assistance in surveillance is the responsibility of the activity authorizing the transmission of the material.

4-1. Conclusion. The primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations cannot guarantee the protection of classified material nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information.

a. You are reminded that any classified instructions you receive must also be protected. **Do not discuss verbal instructions with anyone after you have delivered the material. Do not talk about where you were, what you did, or what you saw.**

b. If you have questions at any time concerning the security and protection of classified and sensitive material entrusted to you, contact your security manager, or the Security Division, DPTMSEC.

Figure K-4. Courier Briefing for CONUS/OCONUS Hand carry of Classified Material

OCONUS Hand Carry Request Form

PART 1: Support Information.

Unit/Activity making request: _____

Date request submitted: _____

Individual(s) to be designated as courier(s):

Name: _____ Rank/Grade: _____

Clearance: _____

Name: _____ Rank/Grade: _____

Clearance: _____

Proposed date(s) of hand carry mission:
_____

Classification of Material: _____

Departure Point: _____ Destination: _____

Intermediate Overnight Stops: _____

_____

Justification for mission: _____

_____

_____

Justification for return mission (if any): _____

_____

_____

AIRLINE SCHEDULE:

Departure Point Time Flight Number
Arrival Point Time

OCONUS Hand carry Request Form (con't)

Storage arrangements during overnight stops in route:

Storage arrangements at destination:

PART II: Mission Evaluation

1. All other means of moving the information/ material have been explored and are not feasible.	Go	No Go
2. Individual(s) has the required security clearance.		
3. Justification for mission and return mission (if any) are adequate.		
4. Airline is a US Carrier, or reviewing official has confirmed US carrier is not available.		
5. Storage on US government facility has been arranged for overnight stops in route and on return, if required.		
6. Storage on US Government facility has been arranged at destination.		
7. Material can be appropriately double wrapped and hand carried by the individual, or it is a bulk item and "last on – first off" arrangements have been made with the airline.		
8. Current intelligence regarding terrorist threat at the destination/transfer points indicates mission can be conducted with a reasonable expectation of success and individual safety.		

PART III: Approval/Disapproval.

1. Mission is approved pending final approval by the MACOM/NERO, through the Security Division, DPTMS.

2. Mission is declined for the following reason(s):

Signature block of approving authority

Figure K-5. OCONUS Hand carry Request Form

DD Form 2501 Record of Issue

Serial #	Issued to	Issue date	Signature Of Courier	Disposition Date	Initials

Figure K-6. DD Form 2501 Record of Issue

Appendix L
Preliminary Inquiries and Security Investigations

L-1. Procedures for the preliminary inquiry

a. The activity head/unit commander, in which an incident of possible loss or compromise of classified information occurs, will designate in writing, within 24 hours or by conclusion of the next duty day, a person to conduct a preliminary inquiry (PI) into the incident, upon written notification from the (CSM) to initiate a PI. The individual designated to conduct the PI, hereafter, referred to as the investigating officer, will have the appropriate security clearance, be senior to everyone known involved in the incident, and not from the division or office in which the incident occurred. A copy of their appointment memorandum will be forwarded to the CSM. Refer to Figure L-1 of this supplement for sample Preliminary Inquiry Appointment Memorandum.

b. The investigating officer will contact the CSM for additional guidance prior to starting the PI.

c. The investigating officer will submit the results of the PI to the activity head/unit commander within 10 working days from the date of appointment. The CSM may grant an extension to this deadline based on extenuating circumstances.

d. Results of the PI will be prepared in the format provided at Figure 10-1, AR 380-5.

e. PI reports will be unclassified whenever possible. However, if it is absolutely necessary, they will be classified to the highest degree of the classified information contained therein, and will contain appropriate classification authority and declassification instructions.

f. The investigating officer will notify the CSM and his/her chain of command if at any time during the PI it appears that deliberate compromise of classified information may have occurred. The CSM will notify the Fort Monroe Resident Office, 902d Military Intelligence (MI) Group. The PI will stop until the 902d MI Group can conduct its investigation. At the conclusion of the MI investigation, the CSM will notify the investigating officer and his/her activity head/unit commander to complete the PI.

g. Within 3 days of receipt of the completed PI report, the activity head/unit commander will forward it with cover memorandum, through command channels, to the CSM. This memorandum will contain the concurrence or nonconcurrence with the findings and recommendations of the investigating officer; proposed corrective actions; determination if an additional investigation is warranted, i.e., AR 15-6. Refer to Figure L-2 of this supplement for sample Preliminary Inquiry Cover Memorandum.

L-2. Procedures for the AR 15-6 Investigation

a. When the CSM, activity head/unit commander, or higher headquarters determines that further investigation is warranted, an investigating officer will be appointed in accordance with AR 15-6.

b. Upon receipt of the DA Form 1574, Report of Proceedings by Investigating Officer/Board of Officers, the CSM will review the report for technical and administrative sufficiency and forward it to the Staff Judge Advocate (SJA) for legal review.

c. Upon completion of legal review, the SJA will return the DA Form 1574 to the appointing authority, through the CSM, with comments and/or recommendations as deemed necessary.

d. Upon receipt of comments and recommendations by the SJA and the CSM, the activity head/unit commander will take appropriate action in section VIII, DA Form 1574, and notify the CSM, accordingly.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Sample Preliminary Inquiry Appointment Memorandum

S: (10 Working Days)

(Office Symbol) (Date)

MEMORANDUM FOR: (Name/Organization)

SUBJECT: Preliminary Inquiry – Possible Compromise of Classified Information

1. You are directed to conduct a preliminary inquiry concerning the facts and circumstances surrounding: _____ _____.

2. The preliminary inquiry will be conducted in accordance with the provisions specified in Chapter 10, AR 380-5 and HQFM supplement 1. The preliminary inquiry report will be prepared in the format provided at Figure 10-1, Chapter 10, AR 380-5. The completed report will be provided to this office NLT COB _____ (10 working days from date of memorandum).

3. You will contact the CSM prior to starting the preliminary inquiry to obtain technical advice and assistance concerning your duties and responsibilities.

(Activity Head/Unit Commander)

Figure L-1. Sample Preliminary Inquiry Appointment Memorandum

Sample Preliminary Inquiry Cover Memorandum

Office Symbol Date

MEMORANDUM FOR Command Security Manager

SUBJECT: Preliminary Inquiry – Possible Compromise of Classified Information

1. I have reviewed the enclosed preliminary inquiry report, and concur with all findings and recommendations contained therein.

----- OR -----

I have reviewed the enclosed preliminary inquiry report, and concur with findings and recommendations contained therein, with the exception of _____ (List each nonconcurrence issue and reason for non-concurrence).

2. In my opinion, additional investigation into this incident is not warranted.

----- OR -----

In my opinion, additional investigation into this incident is warranted. I have appointed (Name/Organization) to conduct a formal investigation, under the provisions of AR 15-6. The results of this investigation will be provided to you, upon completion.

3. The following corrective actions have been implemented to prevent recurrence:

a. _____
b. _____

4. The results of the preliminary inquiry have also been referred to_____ (responsible commander) for appropriate action as he or she deems necessary. Any action taken by the commander will be reported to you, upon completion. (If applicable)

(Appointing Authority)

CF:
CSM, DPTMS

Figure L-2. Sample Preliminary Inquiry Cover Memorandum